Библиографический список

1. Беспалько В.П. Слагаемые педагогической технологии. – М., 1989. – 192 с.

2. Новые технологии в обучении иностранному языку. Электронный ресурс. URL: http://www.langinfo.ru/index.php?sect_id=1042

3. *Янушкевич Ф.* Технология обучения в системе высшего образования. Пер. с польск. – М. Высшая школа. 1986. – 136 с.

Н.А. Руденков

ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННО ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ

nrudenkov@dlink.ru

Представительство «Д-Линк Интернешнл ПТЕ ЛТД», г. Екатеринбург

Количество учебных аудиторий оснащённых компьютерной техникой в учебных учреждениях с каждым годом увеличивается, улучшается качественная составляющая приобретаемой оргтехники, средств визуализации учебного процесса, программного обеспечения и всё это бесспорно положительная тенденция. По оценкам специалистов, каждая учебное учреждение сегодня имеет т.н. «компьютерный класс» (а иногда и не один), кроме того все учебные учреждения имеют подключение к глобальной информационной сети Интернет. Каждое учебное учреждение имеет свой сайт, педагоги активно участвуют в обсуждениях в электронных конференциях, внедряются системы «электронных дневников», «электронных журналов» и пр.

К сожалению, сегодняшние реалии таковы, что критерии оценки использования средств ИКТ учебного учреждения сводятся к количественному перечислению «компьютерных классов», медиа проекторов, электронных досок и пр. Из года в год руководители учебных учреждений планируют в своих бюджетах средства на приобретение пресловутых «компьютерных классов». Их можно понять, ведь нужно ежегодно отчитываться о внедрении современных средств ИКТ в образовательную систему, равно как и о качественном улучшении (благодаря внедрению средств ИКТ) самого процесса образования, и в конечном итоге о реализации федеральных программ связанных с образованием. Однако мало кто из них задумывается о создании в своих учреждениях информационно коммуникационной среды. В данном случае имеется ввиду хотя бы физическое объединение существующих средств ИКТ (персональные компьютеры, оргтехника, медиа проекторы, и пр.) в единую информационную среду (сеть), и разумеется, с последующим развитием этой информационной сети в защищённую, управляемую, структурированную информационно образовательную среду, способную обеспечивать решение текущих и перспективных задач образования.

Не секрет, что не во всех учебных учреждениях существует локальная вычислительная сеть (ЛВС), и ещё большая редкость - ЛВС управляемая и грамотно сконфигурированная. А ведь ЛВС является средой для взаимодействия друг с другом средств ИКТ, и тем основанием (или «скелетом») на базе которого и формируется информационно образовательная среда, «обрастая» в своём развитии новыми педагогическими методами, приёмами применения средств ИКТ, образовательными инициативами. ЛВС является по сути своей «транспортом» для передачи данных, т.е. необходимым условием успешного взаимодействия средств ИКТ учебного (равно как и любого другого) учреждения.

Необходимо однозначно понять–любая образовательная (педагогическая) инициатива, связанная с применением средств ИКТ будет обязательно «буксовать» в случае отсутствия управляемой и защищённой ЛВС учебного учреждения!

Локальная вычислительная сеть образовательного учреждения должна в себя включать как минимум несколько обязательных подсетей, в том числе :

- администрации, куда входят рабочие места руководителя, его заместителей, преподавателей;
- библиотеки, куда входят файл-сервер (электронная библиотека) и рабочие места библиотекаря и читателей;
- бухгалтерия, обособленная подсеть с возможностью авторизованного доступа к ней;
- учебных классов и аудиторий.

Кроме того, должна быть предусмотрена возможность фильтрации и управления потоками данных (трафиком), а значит, сеть должна быть управляемой, и защищённой. Для реализации управления сетевым трафиком, необходимо использовать при построении ЛВС управляемые коммутаторы, активно используя при этом технологии разграничения и контроля трафика.

Для надёжной защиты всей информационно вычислительной сети, в качестве устройства подключения учреждения к Интернет следует применять т.н. межсетевые экраны. Межсетевые экраны - это аппаратные специализированные устройства, предлагающие всестороннюю защиту от несанкционированного доступа в сеть и нежелательного контента, а также от вирусных атак. Например, серия устройств DFL NetDefend UTM оснащены системой обнаружения и предотвращения вторжения злоумышленниками, антивирусом и фильтрацией Web-содержимого для проверки и защиты содержимого. Эти устройства позволяют распознавать угрозы и обеспечивать защиту сети, как против известных, так и против неизвестных сетевых атак. По сути, устройства с таким функционалом по праву можно назвать средством коллективной информационной безопасности (СКИБ). И пренебрегать такими устройствами в информационно вычислительной сети учебного учреждения было бы не разумно.

Такая конфигурация локальной вычислительной сети (имеется ввиду качественный её состав, перечисленный выше) должна считаться минимально необходимой для каждого учебного учреждения, иными словами должна стать типовой конфигурацией информационной сети учебного учреждения. Структурированная, управляемая и защищённая ЛВС учреждения позволит качественно и в полном объёме использовать существующие средства ИКТ, такая сеть позволит без дополнительных затрат планировать и внедрять новые технологии и сервисы.

Например, создание, системы видео наблюдения на базе такой типовой конфигурации не предоставит большого труда, потому что процесс создания системы, по сути, сведётся к подключению IP-видеокамер в рамках существующей ЛВС. В свою очередь, систему видеонаблюдения можно использовать для проведения видео уроков с учащимися по состоянию здоровья отсутствующими на занятиях, или для проведения видео конференций с абонентами других учебных учреждений города, страны и зарубежья.

Без особых проблем в такой сети реализуется сервис IP-телефонии, что позволит, во-первых оснастить внутренней телефонной связью все необходимые помещения учреждения, а во-вторых – отказаться от «лишних», ставших уже не нужными телефонных линий ГТС.

Вместе с тем, важно отметить, что при создании ИОС нельзя полагаться только на техническую составляющую. Важным элементом работоспособности любой информационно вычислительной сети, в том числе и ИОС, является обеспечение информационной безопасности. Особенно актуальным вопрос информационной безопасности становится в свете обеспечения реализации требований Федерального закона РФ от 27.06.2006г. №152 «О персональных данных».

Безопасность информации (данных) – механизм защиты информации (данных), при котором обеспечены её (их) конфиденциальность, доступность и целостность (Национальный стандарт РФ «Защита информации. Основные термины и определения» (ГОСТ Р 50922-2006)).

- Конфиденциальность: доступ к информационным ресурсам и информации только авторизованным пользователям.
- Целостность: неизменность информации в процессе ее передачи или хранения.
- Доступность: свойство информационных ресурсов, в том числе информации, определяющее возможность их получения и использования авторизованными пользователями.

Точками приложения процесса защиты информации к информационной системе являются:

- аппаратное обеспечение (персональные компьютеры и их составные части);
- программное обеспечение (пользовательские программы, исходные, объектные, загрузочные модули; операционные системы и системные программы (компиляторы, компоновщики и др.), утилиты, диагностические программы и т.д.);
- коммуникации (обеспечение передачи и обработки данных через каналы связи и коммутационное оборудование).

Необходимо учитывать, что информационная безопасность – это не только защищенность информации, но и защищённость поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений. Поддерживающая инфраструктура – это системы электро-, тепло-, водо-, газоснабжения, системы кондиционирования и т. д., а также обслуживающий персонал.

Наибольший эффект при обеспечении информационной безопасности достигается тогда, когда все используемые средства, методы и мероприятия объединяются в единый, целостный механизм – систему защиты информации. Функционирование механизма защиты должно постоянно контролироваться, обновляться и дополняться в зависимости от изменения внешних и внутренних условий.

Очевидно, что при создании ИОС учебных учреждений необходимо разработать единые правила и требования направленные на обеспечение информационной безопасности. При проектировании и создании системы информационной безопасности в РФ, прежде всего следует руководствоваться ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью». Данный стандарт

идентичен международному стандарту ISO/IEC 17799-2000 «Information technology. Code of practice for security management» и устанавливает рекомендации по управлению информационной безопасностью.

Этот документ предназначен для обеспечения общих основ при разработке стандартов безопасности и выбора практических мероприятий по управлению информационной безопасностью в организациях на территории РФ и расценивается как отправная точка для разработки необходимых документов и мероприятий под конкретные нужды объекта (предприятия). Не все инструкции и мероприятия, указанные в этом документе, могут быть применимы в каждом конкретном случае. Более того, при реализации конкретной системы информационной безопасности ИОС, возможно, потребуются дополнительные меры, не определенные данным стандартом.

Одной из важных мер организационного характера при формировании системы информационной безопасности, в первую очередь, согласно ГОСТ Р ИСО/МЭК 17799-2005, следует считать разработку политики информационной безопасности.

Политика информационной безопасности разрабатывается и реализуется высшим руководством организации (предприятия, учреждения и т.п.), и должна быть утверждена, документально издана и надлежащим образом доведена до всего персонала.

В этом документе отражаются следующие вопросы:

- определение информационной безопасности, её общие цели и сферы действия, а также раскрытие значимости безопасности как инструмента, обеспечивающего возможность совместного использования информации;
- цели и принципы информационной безопасности, сформулированные руководством;
- классификация и управление информационными активами;
- краткое изложение наиболее существенных для организации правил, принципов и требований безопасности;
- определение общих и конкретных обязанностей сотрудников в рамках управления информационной безопасностью, включая своевременное информирование об инцидентах нарушения информационной безопасности;
- ссылки на документы, дополняющие политику информационной безопасности (детальные процедуры и правила безопасности для конкретных информационных систем, правила информационной безопасности пользователей, документ, закрепляющий за пользователями компьютерную технику, её элементы и периферийные устройства и т.п.);
- определение (назначение) должностного лица, ответственного за реализацию политики информационной безопасности, а также её пересмотр в соответствии с установленной процедурой;
- обеспечение информационной безопасности при наличии доступа к информационным системам;
- вопросы информационной безопасности, связанные с персоналом;
- физическая защита и защита от воздействий окружающей среды объектов информационной безопасности.

Качественная разработка и строгое соблюдение указанных правил – достаточно действенная мера, направленная на то, чтобы привести к минимуму риск утраты

(повреждению) наиболее важной информации и определить объем похищенных сведений, в случае компрометации или утраты.

В качестве одной из мер призванных повысить уровень знаний в вопросах сетевых технологий и применения информационно вычислительных сетей, компания D-Link приглашает учебные заведения принять бесплатное участие в своей программе образования. Разрабатывая собственную программу обучения, компания D-Link придает большое значение работе с учебными заведениями по формированию в них благоприятной информационно-образовательной среды – как в формировании сетевой инфраструктуры, так и методической поддержки процесса обучения сетевым технологиям. Программа D-Link предусматривает теоретическую и практическую подготовку преподавателей и студентов, на безвозмездной основе, по основным направлениям сетевых технологий в очной и дистанционной форме.

Ознакомиться с программой обучения компании D-Link можно на сайте компании http://dlink.ru , в разделе «Обучение», или в офисах компании.

Библиографический список:

1. Сайт компании D-Link. http://www.dlink.ru
2. Национальный стандарт РФ «Информационная технология. Практические правила управления информационной безопасностью» ГОСТ Р ИСО/МЭК 17799–2005.
3. *Руденков Н.А., Долинер Л.И.* «Основы сетевых технологий».

А.А. Рыбанов

ПОДХОДЫ К РАЗРАБОТКЕ WEB-ОРИЕНТИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ МОНИТОРИНГА И УПРАВЛЕНИЯ ПРОЦЕССОМ ПРОХОЖДЕНИЯ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

alexandr@rybanov.ru
Волжский политехнический институт (филиал) ФГБОУ ВПО «ВолгГТУ», Волжский

This article deals with the problems of organization of professional practice. The author suggest web-centric information system to improve the process of students' practice. Increasing of student's work activity in coping with programme of professional practice and intensification of independent work is marked in comparison with the results of professional practice in the previous 2009-2010 academic year.

Одним из условий формирования профессиональной компетентности будущего специалиста является производственная практика – как активный метод обучения, в процессе которого студенты решают реальные практические задачи на производстве.

От эффективности организации производственной практики зависит профессиональный рост студентов как будущих конкурентоспособных специалистов.

Качество производственной практики во многом определяется совокупностью следующих входящих в неё элементов:

1) качество управления производственной практикой;

2) качество образовательных программ и учебно-методических материалов по производственной практике;

3) состав будущих бакалавров, уровень их профессиональной мотивации на избранную профессию;